(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
19. September 2002 (19.09.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/073374 A2

(51) Internationale Patentklassifikation[7]: G06F 1/00

(21) Internationales Aktenzeichen: PCT/DE02/00616

(22) Internationales Anmeldedatum:
20. Februar 2002 (20.02.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 11 756.6 12. März 2001 (12.03.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: INFINEON TECHNOLOGIES AG [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: MEYER, Bernd [DE/DE]; Bert-Brecht-Allee 8, 81737 München (DE). HESS, Erwin [DE/DE]; Gottfried-Keller-Str. 36, 85521 Ottobrunn (DE).

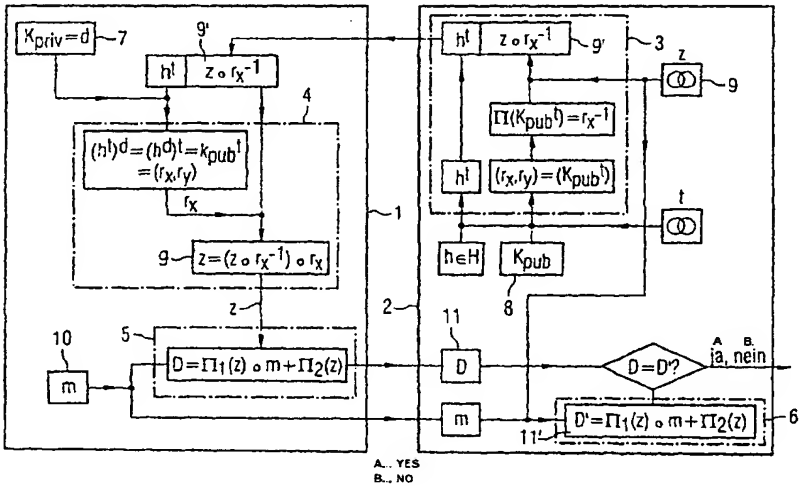
(74) Anwalt: EPPING, HERMANN & FISCHER; Ridlerstr. 55, 80339 München (DE).

(81) Bestimmungsstaaten *(national)*: BR, CA, CN, IL, IN, JP, KR, MX, RU, UA, US.

[Fortsetzung auf der nächsten Seite]

(54) Title: AUTHENTICATION METHOD

(54) Bezeichnung: VERFAHREN ZUR AUTHENTIKATION



(57) Abstract: The invention relates to an authentication and identification method that, on the one hand, uses different codes (7, 8) for the prover (1) and the verifier (2) and, on the other hand, forgoes the use of long-number modulo arithmetic by using simple basic components such as arithmetic operations in finite bodies GF(2^n). A private code (7) is stored in the prover (1) so that the prover can be receive, in an encrypted manner, data elements (9), which are generated as random elements, and can itself be used once again as a code for an authentication method of a data set (10) to be transmitted. The verifier (2) receives the authenticator (11) formed in such a manner and verifies it. If the data set is generated by the verifier (2) and sent to the prover (1), the inventive method can serve to identify the prover (1). This method is particularly advantageous in the area of chip cards due to the fact that the space required thereon can be considerably reduced for the implementation of hardware.

(57) Zusammenfassung: Eine Methode zur Authentikation und Identifikation verwendet einerseits unterschiedliche Schlüssel (7, 8) für den Prover (1) und den Verifier (2), verzichtet andererseits aber auf die Benutzung von Langzahl-Modulo-Arithmetik durch die Verwendung einfacher Grundkomponenten wie beispielsweise arithmetische

[Fortsetzung auf der nächsten Seite]

WO 02/073374 A2

(84) **Bestimmungsstaaten** *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Veröffentlicht:

— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Operationen in endlichen Körpern GF(2n). Ein privater Schlüssel (7) ist beim Prover (1) hinterlegt, so daß dieser als Zufallselemente erzeugte Datenelemente (9) verschlüsselt empfangen und selber wieder als Schlüssel für ein Authentikationsverfahren eines zu übertragenden Datensatzes 10 benutzen kann. Der Verifier (2) empfängt den so gebildeten Authentikator (11) und prüft ihn. Wir der Datensatz vom Verifier (2) erzeugt und an den Prover (1) gesendet, so kann dieses Verfahren zur Identifikation des Provers (1) dienen. Besonders vorteilhaft ist diese Verfahren im Bereich von Chipkarten, da dort der benötigte Platz bei der Hardwareimplementation erheblich reduziert werden kann.